AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated in the following listing of all claims:

1. (***Currently Amended***) A method for controlling reception of messages in an e-mail network, <u>wherein</u> each message is associated with a message sender, <u>the method</u> comprising:

> providing an e-mail relay, the e-mail relay interposed along a message communication path associated with a public network and an e-mail server of the e-mail network;

> the e-mail relay receiving a message intended for a recipient associated with the e-mail network;

> the e-mail relay extracting signature data from the message;

> the e-mail relay ~~validating~~ <u>attempting to validate</u> the signature data; and

> ~~the e-mail relay executing at least one predetermined action in response to determining that the signature data is valid~~

> <u>the e-mail relay performing an action selected from a set that includes at least (i) allowing the message to flow toward the intended recipient via the e-mail server and (ii) diverting the message away from the intended recipient, wherein the selection is based at least in part on a result of the validation attempt.</u>

2. (***Currently Amended***) The method of Claim 1, ~~wherein~~ <u>further comprising:</u>

> the e-mail relay ~~further classifies~~ <u>classifying the message sender based on the</u> signature data <u>and selecting the action at least in part based the classification.</u>

3. (Original) The method of Claim 1, wherein the e-mail relay validates the signature data by employing a validation authority.

4. (Original) The method of Claim 1, wherein said at least one predetermined action comprises allowing the message to proceed to at least one recipient.

5. (*New*) The method of claim 1, further comprising:

> quarantining a diverted e-mail message.

6. (*New*) The method of claim 1, further comprising:

quarantining a diverted e-mail message until the sender completes an enrollment process.

7. (*New*) The method of claim 1, further comprising:

for at least certain categories of e-mail messages received, passing only those e-mail messages for which sender identity is validated based on the extracted signature data.

8. (*New*) The method of claim 10, wherein the categories include one or more of:

e-mail messages having one or more attachments; and

e-mail messages having one or more executables.

9. (*New*) A system for filtering e-mail messages, the system comprising:

an e-mail relay interposed along a message communication path between an e-mail server and a network, the e-mail relay configured to intercept an e-mail message along the message communication path and to extract signature data, if any, from the intercepted e-mail message,

the e-mail relay having an interface for communication with a validation authority and being configured to decide, based at least in part on presence and validation of the extracted signature data, whether the intercepted e-mail message should (i) be allowed to continue along the message communication path toward an intended recipient thereof or (ii) be diverted therefrom.

10. (*New*) The system of claim 9,

wherein, based on the decision, the e-mail relay implements a security policy that, for at least a subset of e-mail messages intercepted, passes only those e-mail messages for which sender identity is validated based on an extracted signature.

11. (*New*) The system of claim 10, wherein the subset includes one or more of:

e-mail messages having one or more attachments; and

e-mail messages having one or more executables.

12. (*New*) The system of claim 9,

wherein, based on the decision, the e-mail relay diverts those messages for which sender identity is unvalidated and initiates a sender enrollment process.

13. (*New*) The system of claim 9,

wherein the decision whether the intercepted e-mail message should be (i) allowed to continue or (ii) diverted is further based on classification of the validated sender identity as trusted or untrusted.

14. (*New*) The system of claim 9,

wherein the e-mail relay is further configured to quarantine a diverted e-mail message.

15. (*New*) The system of claim 9,

wherein the e-mail relay is further configured to quarantine a diverted e-mail message until the sender completes an enrollment process.

16. (*New*) The system of claim 15,

wherein, after successful enrollment of the sender, the e-mail relay associates a valid signature with a diverted e-mail message and passes the previously quarantined e-mail message.

17. (*New*) The system of claim 9,

wherein the intended recipient is an internal recipient, and

wherein the intercepted e-mail message is inbound from the network to the e-mail server.

18. (*New*) The system of claim 9,

wherein the intended recipient is an external recipient, and

wherein the intercepted e-mail message is outbound from the e-mail server to the network.

19. (*New*) The system of claim 9, further comprising one or more of:

the e-mail server; and

the validation authority.

20. (*New*) An e-mail firewall for restricting transmission of e-mail messages between a first site and a plurality of second sites in accordance with a plurality of administrator selectable policies, said firewall comprising:

a simple mail transfer protocol (SMTP) relay for causing said e-mail messages to be transmitted between said first site and selected ones of said second sites; and

a plurality of policy managers, responsive to said SMTP relay, for enforcing administrator selectable policies, said policies comprising one or more source/destination policies, one or more content policies, one or more virus policies, and one or more signature policies, said policies characterized by a plurality of administrator selectable criteria, a plurality of administrator selectable exceptions to said criteria, said policy managers comprising:

an access manager for restricting transmission of e-mail messages between said first site and said second sites in accordance with said one or more source/destination policies;

a content manager for restricting transmission of e-mail messages between said first site and said second sites in accordance with said one or more content policies;

a virus manager for restriction transmission of e-mail messages between said first site and said second sites in accordance with said one or more virus policies; and

a security manager for restricting transmission of e-mail messages between said first site and said second sites in accordance with said one or more signature policies.

21. (*New*) The e-mail firewall of claim 20,

configured to intercept the e-mail messages along a path between the first site and the second sites and to extract signature data, if any, from an intercepted e-mail message,

- 5 -

the e-mail relay further configured to decide, based at least in part on presence and
   validation of the extracted signature data, whether the intercepted e-mail message
   should (i) be allowed to continue along the path toward an intended recipient
   thereof or (ii) be diverted therefrom.

22. (*New*) A computer program product embodied in one or more media and including
instruction executable to cause a computer interposed along a message communication path
between an e-mail server and a network to function as an e-mail relay, the computer program
product comprising:
   executable to intercept an e-mail message along the message communication path and to
      extract signature data, if any, from the intercepted e-mail message; and
   instructions executable to decide, based at least in part on presence and validation of the
      extracted signature data, whether the intercepted e-mail message should (i) be
      allowed to continue along the message communication path toward an intended
      recipient thereof or (ii) be diverted therefrom.